UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN RE HANNAFORD BROS. CO. CUSTOMER DATA SECURITY BREACH LITIGATION	)	MDL Docket No. 2:08-md-1954
JOHN ANDERSON, of Portsmouth, New Hampshire; MICHAEL CYR, of Presque, Isle, Maine; ELIZABETH DOWD, of Fort Myers, Florida; STEVE EARLEY, of Falmouth, Maine; CYNDI and THOMAS FEAR, of Yarmouth, Maine; MARK FOLLANSBEE, of Scarborough, Maine; CARLETON GREELY, of South Portland, Maine; ROBERT HANSON, of Palm Harbor, Florida; PAULINE and BRUCE HATCH, of Harrison, Maine; JOHN and NANCY HUTCHINGS, of Cumberland, Maine; ROBERT JENKINS, of Scarborough, Maine; PAMELA LAMOTTE, of Colchester, Vermont; PAMELA MERRILL, of Sandown, New Hampshire; SSG JESSICA CHOATE and PAMELA WILLIAMS, of Londonderry, New Hampshire; JEANNE SMITH, of Waterville, Maine; EILEEN TURCOTTE, of Litchfield, Maine; and LORI VALBURN, of Essex, Vermont	)	
Plaintiffs,	)	
v.	)	
HANNAFORD BROS. CO., a Maine corporation with its principal place of business at Scarborough, Maine	)	
Defendant.	)	

CONSOLIDATED CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED
INJUNCTIVE RELIEF SOUGHT

TABLE OF CONTENTS

Plaintiffs above named, on behalf of themselves and all other persons similarly situated, allege on information and belief (except as to paragraphs 35 through 51, which are alleged on the respective Plaintiffs' personal knowledge), including a review of publicly available information and advice of computer security experts, as follows:

Certain plaintiffs named in the actions consolidated in this Consolidated Class Action Complaint are not set forth as named plaintiffs here. Those parties do not dismiss any claims or waive any rights. The Plaintiffs named herein are competent to assert the claims set forth herein and can adequately represent the class, including all absent class members.

PRELIMINARY STATEMENT

1. This action is brought to obtain redress for losses and damages sustained by the Plaintiffs and other members of the Class (as hereinafter defined) as a result of the failure of the Defendant to maintain the security of private and confidential financial and personal information of Defendant's credit and debit card customers at Hannaford and Sweetbay supermarkets in Maine, New Hampshire, Vermont, Massachusetts, New York and Florida, and at certain independently owned stores for which the Defendant provided electronic payment services, over a period of approximately three months from December 7, 2007 to March 10, 2008 (the “Class Period”).

2. The Plaintiffs were customers of these stores during the Class Period. In the course of making purchases at these stores during the Class Period, Plaintiffs made use of debit cards and credit cards issued by financial institutions to access their bank accounts or create credit relationships.

3. In making these purchases, Plaintiffs and Class members were requested

by Defendant to confide and make available to Defendant, its agents and employees, private and confidential debit and credit card information, some of which was encoded on their cards, including their names, card numbers, expiration dates, PIN numbers, and security codes.

4. This information was entrusted to Defendant solely for the purpose of effectuating payment for purchases and with the expectation and implied mutual understanding that Defendant would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

5. On or about December 7, 2007, wrongdoers obtained access to Defendant's information technology systems and, until containment of this security breach on or about March 10, 2008, stole private and confidential debit card and credit card information, including up to an estimated 4.2 million debit card and credit card numbers, expiration dates, security codes, PIN numbers and other information, belonging to Plaintiffs and other customers of Defendant who had used debit cards and credit cards to transact purchases at supermarkets owned or operated by Hannaford and Sweetbay in the Northeast and Florida and at independently owned grocery stores for which Hannaford provided electronic payments services.

6. As a result of this breach of security, Plaintiffs' and other Class members' debit cards and credit cards were exposed and subjected to unauthorized charges; their bank accounts were overdrawn and credit limits exceeded; they were deprived of the use of their cards and access to their funds; their preauthorized charge relationships were disrupted; they were required to expend time, energy and expense to address and resolve these financial disruptions and mitigate the

consequences; they suffered consequent emotional distress; and their credit and debit card information is at an increased risk of theft and unauthorized use.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs; at least one Plaintiff has citizenship diverse from the Defendant; and there are more than 100 class members.

8. Venue is proper in this Court under 28 U.S.C. § 1391(a)(2), because Defendant's primary place of business is within this District and the conduct of the Defendant upon which the Plaintiffs' claims are based occurred primarily within this District.

PARTIES

9. Plaintiffs are residents of the following towns and states:

i. John Anderson is a resident of Portsmouth, New Hampshire;

ii. Michael Cyr is a resident of Presque Isle, Maine;

iii. Elizabeth Dowd is a resident of Fort Myers, Florida;

iv. Steve Earley is a resident of Falmouth, Maine;

v. Cyndi and Thomas Fear are residents of Yarmouth, Maine;

vi. Mark Follansbee is a resident of Scarborough, Maine;

vii. Carleton Greeley is a resident of South Portland, Maine;

viii. Robert Hanson is a resident of Palm Harbor, Florida;

ix. Pauline and Bruce Hatch are residents of Harrison, Maine;

x. John and Nancy Hutchings are residents of Cumberland, Maine;

xi. Robert Jenkins is a resident of Scarborough, Maine;

xii. Pamela LaMotte is a resident of Colchester, Vermont;

xiii. Pamela Merrill is a resident of Sandown, New Hampshire;

xiv. Jessica Choate is a Staff Sergeant on active duty in the U.S. Army who resided during the Class Period with her mother, Pamela Williams, in Londonderry, New Hampshire;

xv. Jeanne Smith is a resident of Waterville, Maine;

xvi. Pamela Williams is a resident of Londonderry, New Hampshire;

xvii. Eileen Turcotte is a resident of Litchfield, Maine;

xviii. Lori Valburn is a resident of Essex, Vermont.

10. Defendant Hannaford Bros. Co. ("Hannaford") is a corporation organized under the laws of the State of Maine, with its principal place of business in Scarborough, Maine. Hannaford owns and operates supermarkets in Maine, New Hampshire, Massachusetts, Vermont, and New York.

11. Kash N' Karry Food Stores, Inc. ("Kash N' Karry") is a Delaware corporation, which owns and operates supermarkets in the State of Florida under the name of "Sweetbay".

12. Hannaford and Kash N' Karry are both wholly-owned subsidiaries of Delhaize America, Inc. ("Delhaize"), a Delaware corporation with its principal place of business in Salisbury, North Carolina.

13. During the time periods relevant to this Consolidated Class Action Complaint, Hannaford provided information technology and data processing services to Kash N' Karry, including the processing of customer debit card and credit card payments.

14. Hannaford also provided electronic payment processing services to a number of independently owned stores in various states.

15. Hannaford has stipulated and agreed that judgment may be entered against it based on any liability of Kash N' Karry, Delhaize, and such independently owned stores that may be established in this case. In the interest of simplicity and manageability, those entities have not been joined as defendants in this Consolidated Class Action Complaint.

16. The terms "Hannaford" and "Defendant" should be interpreted to include Delhaize, Kash N' Karry, and such independently owned stores as the context requires.

FACTS

17. On March 17, 2008, Hannaford publicly announced for the first time that between December 7, 2007 and March 10, 2008, the security of its information technology systems had been breached, leading to the theft of as many as 4.2 million debit card and credit card numbers belonging to individuals who had made purchases at more than 270 of its stores, including 165 Hannaford stores in New England and New York, 106 Sweetbay stores in Florida, and an additional number of independently owned grocery stores in various states for which Hannaford provided electronic payment services, and that it had already received reports of

approximately 1,800 cases of fraud resulting from the theft of those numbers.

18. For some period of time before, during and after the Class Period, Defendant has invited customers, including Plaintiffs and the Class members, to make use of their debit cards and credit cards to pay for purchases at Hannaford supermarkets and other stores for which Hannaford provided electronic payment services.

19. Based on this invitation, Plaintiffs and the Class members made use of their debit cards and credit cards to pay for their purchases at such stores during the Class Period.

20. In the course of making such purchases and paying for them, Class members confided their private and confidential debit card and credit card information to Defendant solely for the purpose of enabling Defendant to effectuate such payments. Such data was confided based on express and implied representations by Defendant and on the expectation and implied mutual understanding that the data confided would be protected and safeguarded from access by unauthorized individuals.

21. During the Class Period, Defendant failed to adequately safeguard and protect the private and confidential debit card and credit card information of Plaintiffs and Class members, so that wrongdoers were able to obtain access to such data within Defendant's information technology systems or in the course of transmission of the data to financial institutions.

22. Lack of adequate security in Defendant's information technology systems enabled the wrongdoers to place foreign software, known as malware, on

Defendant's information technology systems, which then provided the wrongdoers with access to customer debit card, credit card, and possibly other electronic information then in transit or temporarily stored on the system, and then diverted this information to the wrongdoers.

23. Defendant did not monitor their information technology system for the presence of foreign software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue unnoticed for more than three months.

24. Defendant's information technology system had multiple security shortfalls, including, but not limited to:

i. lack of proper monitoring solutions;

ii. failure to encrypt internal network traffic flowing between store and processor;

iii. point-of-sales systems that were open to attack;

iv. insecure wireless connections; and/or

v. remote access deficiencies.

25. On February 27, 2008, Visa notified Hannaford that a pattern of unusual fraudulent credit card activity involving customers who had made debit card and credit card transactions at Hannaford stores indicated that its information technology system had been breached.

26. On March 8, 2008, Hannaford computer technicians discovered the means by which wrongdoers had obtained unauthorized access to confidential customer data in its system.

27. The security breach was not contained until March 10, 2008. On that day, Defendant notified certain financial institutions of the data intrusion.

28. Although Defendant first became aware of the breach of its information technology system as early as February 27, 2008, Defendant failed to disclose publicly that customers' private and confidential financial and personal information had been accessed and stolen until Hannaford announced the data intrusion publicly on March 17, 2008.

29. The wrongdoers who obtained such access and stole customers' data and their transferees misused this data by making unauthorized charges against the debit card and credit card accounts of Plaintiffs and other Class members. By the time Hannaford publicly announced the security breach, over 1,800 such charges had already been identified. Since then many more have taken place.

30. Defendant's initial public disclosure of the theft of its customers' personal and financial data was incomplete. In "[a] Message From Hannaford CEO Ron Hodge" posted on its website on March 17, 2008, Hannaford stated:

> Hannaford has contained a data intrusion into its computer network that resulted in the theft of customer credit and debit card numbers. No personal information, such as names or addresses, was accessed. Hannaford doesn't collect, know or keep any personally identifiable customer information from transactions.

31. Hannaford's initial posting failed to disclose that additional information including card expiration dates and security codes, as well as, positive authorization results had been stolen or that this information was sufficient to enable the wrongdoers to make fraudulent charges to cardholder accounts. The initial posting also failed to disclose that as of the time Hannaford became aware of the theft over

1,800 fraudulent charges had been identified and that many more could be expected. The initial posting failed to disclose the time period during which customer data was exposed to theft, the number of customers affected, and the independent stores whose customers' data had been implicated in the breach.

32. Defendant's notification to its customers concerning the theft of their data was limited to the initial announcement, postings on its website, and notices posted in its stores. Defendant has not attempted to notify its customers individually through their card issuing financial institutions nor has it undertaken any public advertising campaign calculated to reach its customer base in the various states in which it does business.

33. Defendant still has not advised each of its customers of exactly what private and confidential financial and personal information belonging to each of them was stolen or exposed to theft as a result of this data breach. Nor has Defendant taken any other steps to assist customers whose credit and debit card data was stolen by provision of credit or card monitoring, reimbursement of out-of-pocket expenses, or compensation for time, effort, disruption and emotional distress occasioned by the breach of its information technology system.

34. Following Hannaford's announcement of the data breach:

i. some financial institutions immediately cancelled customers' debit and credit cards and issued new cards, while others waited for evidence of unauthorized activity to take action;

ii. financial institutions who did not immediately cancel customers' cards monitored customer accounts for unusual activity and

cancelled cards immediately upon being aware of apparent fraudulent charges or attempts to make apparently fraudulent charges, in many cases, without the knowledge of the customer;

iii. customers suffered unauthorized charges to their debit card and credit card accounts;

iv. customers' accounts were overdrawn and their credit limits exceeded by virtue of unauthorized charges;

v. customers were deprived of use of their cards for appreciable periods of time and were unable to access their accounts or their funds;

vi. customers lost accumulated miles and points toward bonus awards and were unable to earn points during the interval their cards were inactivated;

vii. customers who requested that their cards be cancelled were required to pay fees to issuing banks for replacement cards;

viii. customers who had registered their cards with online sellers were required to cancel and change their registered numbers;

ix. customers who had given creditors pre-authorization to charge their debit cards or credit cards for recurring payments were required to change the pre-authorizations;

x. customers were placed in non-payment status by virtue of their cards being overdrawn or abruptly cancelled and were required to pay penalties and service reinstatement fees;

xi. customers purchased identity theft insurance and credit monitoring services to protect themselves against possible consequences of the breach;

xii. customers suffered emotional distress as they were forced to cope with the unauthorized charges and other consequences of Defendant's data breach; and

xiii. some customers are still not aware of the data breach or that their data has been compromised, have not been monitoring their accounts for fraudulent charges, and are hence particularly susceptible to or have already sustained fraudulent charges to their accounts for which they have not sought reimbursement.

SPECIFIC REPRESENTATIVE PLAINTIFF ALLEGATIONS

35. Plaintiff John Anderson made purchases at a Hannaford store in Wells, Maine during the Class Period using a debit and credit card. Following the announcement of the data theft, he consulted his bank and was told that he should continue to use his card and see how matters "played out." Somewhat later, his bank notified him that his card had been compromised, the card was cancelled, and a new card was issued. Plaintiff Anderson was deprived of the use of the card for several days. He was forced to get in touch with several preauthorized creditors and arrange new pre-authorizations. In at least one case, he failed to reach a preauthorized internet service provider in time and was threatened with termination of service and forced to pay a reinstatement penalty for late payment. He was also forced to change card numbers registered with online businesses such as Amazon,

eBay, and Apple iTunes.

36. Plaintiff Michael Cyr used his Sears Mastercard and his GM Mastercard to make purchases at a Hannaford store in Presque Isle, Maine during the Class Period. He habitually used the Sears card to make many purchases for his businesses so that he could earn Sears points to be redeemed for merchandise at Sears or cash. Sears advised him by telephone that the card was being cancelled. He was required to call all of his business and personal vendors to give them the number of his GM Mastercard to cover purchases and payments during the interval until a new Sears card would be issued. After he and his bookkeeper had contacted all suppliers and other pre-authorized payees, he received a call cancelling the GM Mastercard as well, necessitating another round of communications. During the interval when he was unable to use his Sears card, he was deprived of the opportunity to earn Sears points on his purchases and payments.

37. Plaintiff Elizabeth Dowd used her Florida Gulf Bank Mastercard debit card to make purchases at a Sweetbay store in Fort Myers, Florida during the Class Period. On or about March 2008, her card was cancelled by the issuing bank and she was deprived of access to her funds until a replacement card was issued. She was also required to expend time and effort to change pre-authorizations. The card was again cancelled on or about April of the same year and she was once again without access to her funds until a replacement card was issued and once again was required to notify creditors and change pre-authorizations.

38. Plaintiff Steve Earley used his credit and debit cards to make purchases at a Hannaford store in Falmouth, Maine during the Class Period. On or about May

2008, he discovered that two fraudulent charges totaling approximately $300.00 had been made to his Discover credit card account at gas stations in Georgia. At the card company's insistence, his card was cancelled and a new account was opened. The card company did not transfer accumulated cash back bonus reward points to his new account and he lost them. It took approximately two weeks before Plaintiff Earley received his replacement credit card, during which time he was unable to accumulate cash back bonus reward points on purchases. A preauthorized charge for a gym membership and motor vehicle electronic toll account were also disrupted. On April 11, 2008, his debit card was also cancelled by the issuer Infinity Federal Credit Union due to the Hannaford breach.

39. Plaintiffs Cyndi and Thomas Fear used their debit card issued by Key Bank to make purchases at a Hannaford store in Yarmouth, Maine during the Class Period. When they learned of the data breach, Plaintiffs requested that their card be cancelled and a new one issued. Plaintiffs were required to pay a $20.00 fee for the replacement card.

40. Plaintiff Mark Follansbee and his wife Alberta used their MBNA Visa card and Citibank Mastercard to make purchases at a Hannaford supermarket in Scarborough, Maine during the Class Period. When the Hannaford data security breach became known, the cards were quickly cancelled by the issuers. Mr. Follansbee was required to notify creditors holding pre-authorizations and in at least one case was required to pay a fee to change the pre-authorization. Mr. and Mrs. Follansbee had booked travel reservations using the cancelled cards and when they were traveling a hotel declined to honor a reservation on the ground that the card

had been cancelled.

41. Plaintiff Carleton Greely used debit cards issued by TD Banknorth and Town and Country Credit Union to make purchases at the Hannaford store in South Portland, Maine on a regular basis during the Class Period. Between December 2007 and February 2008, he became aware of several unauthorized charges on his bank statement amounting to between $1,000.00 and $2,000.00 on both cards. He changed his account several times, but continued to experience unauthorized charges. Because his bank account was almost continuously overdrawn, resulting in substantial overdraft fees, he was required to get a bank loan to cover his expenses. Each time a card was cancelled and changed he was required to get in touch with multiple pre-authorized payees to change pre-authorizations.

42. Plaintiff Robert Hanson used his Mastercard debit card to make purchases at a Sweetbay supermarket in Florida during the Class Period. On February 16, 2008, an unauthorized cash withdrawal of $422.00 was made against his account at an ATM in Chicago, Illinois. It took significant time and effort to convince the bank to remove the charge and replace the card.

43. Plaintiffs Pauline and Bruce Hatch each had a debit card issued by Key Bank to access their joint account at the bank. They used their cards to make purchases at a Hannaford store in Oxford, Maine during the Class Period. Following the announcement of the Hannaford data breach, they called their bank on a Saturday morning to see if their account had been affected. They were told that their account was overdrawn and that they did not have access to any funds. It was not until Monday that they were able to visit the bank and ascertain that

unauthorized charges had been made against both of their cards in Austin and San Antonio, Texas, which resulted in overdrawing their account. They were deprived of access to their funds for a period of approximately two weeks while new cards were issued. To this day, they remain apprehensive about using their cards to make purchases.

44. Plantiffs John and Nancy Hutchings used their Bank of America credit card on which they earned reward points to make purchases at a Hannaford store in Falmouth, Maine during the Class Period. On March 14, 2008, Mr. and Mrs. Hutchings received a call from Epson Printing requesting verification of the last four digits of the card and the shopping address for a purchase of $1,649.00. They realized that this was an attempt at a fraudulent purchase, which was listed on their account as "pending." The card was cancelled, and Mrs. Hutchings lost a large number of reward points that otherwise would have been earned on the card from charges during a business trip that took place right after the card was cancelled and before it was replaced.

45. Plaintiff Robert Jenkins used a Discover credit card to make purchases at a Hannaford store in Scarborough, Maine during the Class Period. Although his card was replaced in March 2008, he was notified that charges had been made to his old card after the issuance of his new card. He was required to expend time and effort to convince Discover that the charges were unauthorized and should be removed from his account.

46. Plaintiff Pamela LaMotte used her Capital One Mastercard credit card and her Visa Aspire credit card to make purchases at a Hannaford store in South

Burlington, Vermont on several occasions during the Class Period. Her July 2008 statement showed two charges for $100.00 each in Baltimore, Maryland on the Capitol One account, which put her $142.00 above her credit limit. She disputed these charges as unauthorized, but was required by Capitol One to pay the amount in excess of her credit limit, as well as, overdraft fees and penalties pending resolution of the dispute. The charges remained on her account and she is required to pay interest on them. More recently, the account was sent to collection and she has been forced to set up a payment plan. On the Visa card, she was notified by her bank that her card information may have been compromised and that the bank was monitoring her account for strange activity. Her July and August 2008 statements showed five different charges from Florida locations, which she has disputed as unauthorized. The card has been replaced, but the unauthorized charges remain on her account despite her efforts to have them removed and she has received a letter from Visa stating that payment is overdue and threatening to send the account to collection.

47. Plaintiff Pamela Merrill used a debit card to make purchases at a Hannaford store in East Hampstead, New Hampshire during the Class Period. On August 6, 2008, she noticed a charge totaling $205.50 from Madrid, Spain, and later that same day saw two "pending" charges from Paris, France, all of which were made to her debit account and were unauthorized. She immediately notified the bank. The charge from Spain drained her account and resulted in overdraft fees. On August 14, 2008, she received a "temporary credit" to her debit account pending her bank's investigation into the charges. She was unable to use her account during

the investigation, because any money she deposited into the account would have been absorbed by the overdraft fees. She also had preauthorized payment arrangements with her life insurance company and NetFlix, which she was required to reschedule in order to avoid additional overdraft fees.

48. Plaintiff Pamela Williams is a resident of New Hampshire. Plaintiff Jessica Choate is a Staff Sergeant (SSG) on active duty in the U.S. Army whose legal residence is in Michigan, but was living with her mother, Plaintiff Williams, in Londonderry, New Hampshire during the Class Period. Plaintiff Williams was a secondary card holder on the Visa debit card issued by the United Services Automobile Association (USAA) military bank to her daughter, Plaintiff Choate. Plaintiffs Williams and Choate used their cards to make purchases at Hannaford stores in Londonderry and Derry, New Hampshire during the Class Period. When Plaintiff Choate was sent to Keesler Air Force Base in Biloxi, Mississippi to undergo eye surgery, Plaintiff Williams accompanied her to offer support and assistance. While on the military base, Plaintiff Williams went to a base salon for a manicure. When she went to pay with the USAA Visa card, the charge was declined. The salon attendants threatened to call the Military Police. Misuse of a debit card by a Noncommissioned Officer (NCO) violates the NCO Creed. After explaining her understanding that the account had sufficient funds, Plaintiff Williams assured the salon staff that she would get money to cover the charge. The salon staff gave Plaintiff Williams twenty four hours to remedy the situation and demanded that she turn over her military identification card until the bill was paid in full. After leaving the salon, Plaintiff Williams contacted USAA and learned that their joint account was

$700.00 overdrawn and that there were multiple fraudulent charges for $99.99 on the account for gas purchases in New York. Plaintiff Williams was forced to obtain a $500.00 loan from her father by wire transfer between Navy Federal Credit Union accounts that each of the family members maintain. It took several days before the stolen money was reimbursed and replacement cards were issued for their compromised USAA account.

49. Plaintiff Jeanne Smith used a debit card issued by Key Bank to make purchases at a Hannaford store in Waterville, Maine on several occasions during the Class Period. She learned that her account at Key Bank had been overdrawn by unauthorized purchases in Florida. While the bank was investigating the unauthorized charges, she was deprived of access to her funds and the use of her card for several weeks. Overdraft notices continued to arrive from the bank as additional unauthorized transactions occurred. She is still wary of using her replacement card.

50. Plaintiff Eileen Turcotte and her husband, Richard Turcotte, used a credit card issued by Capitol One in the name of Plaintiff Turcotte to make purchases at Hannaford stores in Maine during the Class Period. When she heard of the Hannaford breach, Plaintiff Turcotte contacted her bank and was told by the bank to continue to use the card and look out for unauthorized charges. Between June 20 and June 24, 2008, there were five fraudulent charges made against Plaintiff Turcotte's card in Georgia and Florida, which caused the bank to cancel the card. For a period of ten days, the Turcottes had no use of the card or any replacement card and were unable to charge purchases.

51. Plaintiff Lori Valburn used her debit and credit cards issued by the Vermont State Employees Credit Union and her Discover Card credit card to make purchases at Hannaford stores near Burlington, Vermont during the Class Period. In April 2008, she reviewed her Discover Card statement and learned that an unauthorized cash withdrawal for $500.00 had been made against her account on March 19, 2008 in Indiana. She called the issuers of all her cards and had them cancelled and replaced. She also spoke with the fraud unit at Discover Card. She was without her canceled cards for approximately 7-10 days. Due to the uncertainty and threat of further unauthorized use of her accounts, she purchased identity theft insurance through Discover Card at a cost of $2.99 per month.

INJURY AND DAMAGES

52. As a direct and proximate result of Defendant's failure to maintain the security of its customers' private and confidential financial and personal data, Plaintiffs and Class members suffered a disruption of their financial affairs and endangerment of their financial assets and resources. They have had to expend time and effort to address, correct, repair, and/or mitigate the consequences of the disruption of their financial affairs and to mitigate and avert the harm threatened to their financial assets and resources, including their credit reputations. They have incurred out-of-pocket loss and damage. They have experienced emotional distress. They remain exposed to the risk of fraud in cases in which compromised debit and credit cards have not been cancelled.

53. The ways in which Plaintiffs and Class members have suffered disruption of their financial affairs and have had to expend time and effort to mitigate the

consequences thereof include, but are not limited to:

i. their debit cards and credit cards were cancelled without notice by issuing financial institutions, or they took preventative action to cancel the cards themselves, depriving them of the use of their cards for appreciable lengths of time;

ii. their bank accounts were overdrawn and credit limits exceeded by unauthorized and fraudulent charges;

iii. they had to identify the fraudulent charges and convince their issuing banks to reverse the charges or restore funds paid to wrongdoers;

iv. they were deprived of access to and the use of their funds during the interval until the fraudulently withdrawn funds were restored by their financial institutions;

v. they took steps to protect their credit, including obtaining credit reports, placing fraud alerts with credit agencies, and purchasing credit monitoring and identity theft insurance;

vi. they were forced to obtain cash and make payments over-the-counter and by other less convenient means after cancellation of their cards and before the issuance of replacement cards;

vii. their preauthorized charges in favor of third-party payees were disrupted and they were required to change preauthorizations to new cards;

viii. they had to change card registrations with on-line merchants and

other payees with whom their credit and debit cards had been registered to facilitate electronic purchases and payments; and

ix. they had airline and hotel reservations cancelled because they had been made on cards that were cancelled.

54. The out-of-pocket loss and damage the Plaintiffs and Class members have incurred include, but are not limited to:

i. unauthorized charges that have been made to their accounts;

ii. unauthorized charges that were not noticed by customers who were not aware that their card numbers were compromised or failed to detect the charges on their statements have been paid or withdrawn from such customers' accounts;

iii. fees, penalties, reinstatement charges, and other consequences of defaults in pre-authorized payments resulting from cancellation of their cards by issuing institutions;

iv. fees paid by customers who sought to cancel their cards and obtain replacement cards to protect themselves from potential unauthorized charges;

v. fees to purchase credit reports, to arrange for credit monitoring, and to purchase identify theft and overdraft insurance;

vi. costs of travel, phone, postage, and other expenses dealing with card issuers in connection with unauthorized charges and replacement cards;

vii. fees for over-the-counter cash withdrawals, checks written, wire

transfers and other transactions, during the period they were deprived of the use of their cards; and

viii. loss of accumulated reward points, airline miles, and similar benefits upon cancellation of their cards and loss of the opportunity to earn such benefits during the interval before they obtained replacement cards.

55. The ways in which Plaintiffs and Class members have been subjected to emotional distress include, but are not limited to:

i. they have experienced uncertainty and apprehension about potential fraudulent charges against their credit card and bank accounts and other misuse of their private and confidential financial and personal information by wrongdoers;

ii. they have experienced stress and worry from strained finances caused by unauthorized charges overdrawing their accounts and exceeding their credit limits, depriving them of access to their funds;

iii. they have been embarrassed and humiliated when their debit cards and credit cards were declined when they attempted to make payments at stores, restaurants, and to other payees, and when they found that reservations that had been made on their cards had been cancelled, because the cards had been cancelled by the issuers, or their bank accounts had been overdrawn or credit limits exceeded as a result of fraudulent charges; and

iv. they have experienced continuing apprehension and insecurity about using their cards.

56. Class members whose debit cards and credit cards were compromised and have not been cancelled remain at risk of fraudulent use of their card data. To date, the wrongdoers have not been caught and the customer data stolen has not been retrieved. Fraudulent charges and attempts to charge on credit and debit card numbers stolen from Hannaford continue to this day. Such data is often "warehoused" by thieves and not used for a year or more after it is stolen, by which time card issuers typically cease monitoring the accounts for fraudulent activity. Some customers do not know of the data security breach or that their cards were compromised and are hence particularly susceptible to future loss.

CLASS ACTION ALLEGATIONS

57. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(2) and (b)(3) on behalf on themselves and all other persons similarly situated.

58. The Class consists of:

i. all persons or entities residing in the United States

a. who made purchases at stores owned or operated by Hannaford Bros. Co. or Kash N' Karry Food Stores, Inc., and/or at independently owned stores for which Hannaford Bros. Co. provided electronic payment services during the period from December 7, 2007 through March 10, 2008, using debit and/or credit cards, and

b. other holders of additional cards on the same accounts; and

ii. whose debit and/or credit card numbers, expiration dates and/or security codes were stolen.

59. The Class does not include the Court, the U.S. Magistrate Judge, counsel for any party, any of their employees or immediate family members, the Defendant, any director, officer or employee of the Defendant, or any of their immediate family members.

60. The exact number of Class members and their identities are unknown at this time. However, since as many as 4.2 million debit card and credit card numbers of Defendant's customers were stolen, the Class members are so numerous that joinder of all individual Class Member is impracticable.

61. Questions of law and fact common to all Class members predominate over any questions affecting only individual members, including the following:

i. Whether Defendant acted negligently in failing to properly safeguard Class members' financial and personal data;

ii. Whether Defendant failed to adequately notify Class members of the compromise of their private and confidential financial and personal data;

iii. Whether Defendant assumed a fiduciary duty and/or confidential relationship to Class members when they entrusted Defendant with their private and confidential financial and personal information to effect purchases;

iv. Whether Defendant breached express or implied contracts with Class members by failing to properly safeguard their private and confidential financial and personal data and by failing to notify them of the breaches of its computer data systems and the nature and extent of their data that had been stolen as soon as practicable after such breaches were discovered;

v. Whether Defendant impliedly warranted to Class members that its electronic payments processing and information technology systems were fit for the purpose intended, namely the safe and secure processing of electronic payment transactions, and whether such warranty was breached;

vi. Whether Defendant should be held strictly liable for the injuries suffered by Class members resulting from failure to maintain the confidentiality of their financial and personal data; and

vii. Whether Hannaford violated the Maine Unfair Trade Practice Act by failing properly to safeguard customers' private and confidential financial and personal data and by failing to notify them of the breaches of its computer data systems and the nature and extent of their data that had been stolen as soon as practicable after such breaches were discovered.

62. Plaintiffs' claims are typical of the claims of all Class members, because all such claims arise from the same set of facts regarding Defendant's failure:

i. to protect Plaintiffs' and Class members' private and confidential financial and personal data;

ii. to discover and remediate the security breach of their computer systems more quickly; and

iii. to disclose to Plaintiffs and Class members in a complete and timely manner information concerning the security breach and the theft of their private and confidential financial and personal data.

63. Plaintiffs have no interests that are antagonistic to the interests of other Class members.

64. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel for the prosecution of this case as a class action.

65. Defendant has acted and refused to act on grounds that apply generally to the Class, so that injunctive or declaratory relief is appropriate respecting the class as a whole.

66. This class action is superior to other available methods for fairly and efficiently adjudicating Class members' claims because:

i. the class is readily definable and prosecution of this action as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual cases;

ii. the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications, which could establish incompatible standards of conduct for the Defendant or allow some Class members' claims to affect adversely other Class members' abilities to protect their interests;

iii. this forum is an appropriate one in which to concentrate the litigation since Hannaford is located here and its conduct giving rise to Plaintiffs' and Class members' claims occurred here; and

iv. the case is manageable as a class action.

COUNT I – BREACH OF IMPLIED CONTRACT

67. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

68. When they confided their private and confidential debit card and credit card information to Defendant in order to make purchases at Defendant's stores, Plaintiffs and Class members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect all such information and to notify them that the confidentiality of such information was compromised.

69. Plaintiffs and Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract with Defendant.

70. Defendant breached the implied contracts they had made with Plaintiffs and Class members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information.

71. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of Defendant's breaches of these implied contracts.

COUNT II - BREACH OF IMPLIED WARRANTY

72. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

73. Defendant provided for its customers an electronic payment processing system consisting of payment terminals, computer servers, an electronic network,

with associated computer software and hardware to enable those customers who wished to pay by debit card or credit card to make payment for purchases at Hannaford and required all such customers to use such system for such purchases. The use of this system by Defendant's customers was for the benefit of Defendant, as well as, customers.

74. Defendant gave each customer who used such system an implied warranty that such system was fit for its intended purpose, namely the safe and secure processing of credit and debit card payment transactions.

75. During the Class Period, such warranty was breached in that such system was not fit for its intended purposes, namely the safe and secure processing of credit and debit card payment transactions and, in fact, allowed wrongdoers to steal customers' confidential personal and financial data.

76. Plaintiffs and Class members were damaged by such breach of warranty in the manner alleged herein.

COUNT III – BREACH OF DUTY OF A CONFIDENTIAL RELATIONSHIP

77. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

78. Plaintiffs and Class members entrusted private and confidential financial and personal information to the Defendant at Defendant's request and placed trust and confidence in the Defendant in order to make payments to Defendant.

79. Defendant had the benefit of a disparity of position and control and Plaintiffs and Class members placed trust and confidence in Defendant.

80. Defendant had a duty to maintain the confidentiality of the private and

confidential financial and personal information, to safeguard and protect it from misuse by unauthorized persons and, once it learned of any security breach, to keep Plaintiffs and Class members fully apprised of the nature, extent, and relevant facts of the breach and loss of private and confidential information.

81. Defendant breached its duty by failing to take necessary measures to maintain the confidentiality of Plaintiffs' and Class members' private and confidential financial and personal information and to safeguard and protect it from misuse by unauthorized persons.

82. Defendant also breached its duty by failing and continuing to fail to adequately disclose to Plaintiffs and Class members sufficient information regarding the nature, extent, and relevant facts of the breach and the loss of private and confidential information.

83. Defendant abused its superior position in order to, among other things, avoid adverse effects to its business, maintain positive public relations, and retain Plaintiffs and Class members and other customers and entice them to continue shopping and making debit card and credit card transactions in its stores.

84. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of Defendant's breach of its duty of a confidential relationship.

COUNT IV - FAILURE TO ADVISE CUSTOMERS OF THE THEFT OF THEIR DATA

85. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

86. By soliciting and receiving its customers' private and confidential financial

information, including their credit and debit card numbers, expiration dates, and security codes, for the purposes of effectuating payment for purchases at its stores, Defendant undertook a duty to advise its customers promptly and in a complete and accurate manner if the private and confidential data confided to it were compromised or stolen.

87. Upon their discovery of the security breach of their information technology systems and the theft of Plaintiffs' and Class members' private and confidential financial and personal information, Defendant was required by this duty to disclose to each customer whose data was stolen or exposed to theft in a complete and timely manner the nature and extent of such exposure or theft, so that Plaintiffs and Class members could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change account numbers on compromised cards, change pre-authorizations to prevent payment being declined on overdrawn or cancelled cards, and monitor their account information and credit reports for fraudulent activity.

88. Defendant breached this duty by failing and continuing to fail to notify Plaintiffs and Class members in a complete, adequate and timely manner that Defendant's computer systems had been compromised and the precise nature and extent of their customers' data that had been stolen.

89. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of this failure to disclose.

90. Defendant's failure completely and adequately to notify its customers is ongoing, and the prevention of future damage from such failure warrants injunctive relief.

COUNT V - STRICT LIABILITY

91. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

92. Defendant failed adequately to safeguard the private and confidential financial and personal information of their customers entrusted to it in the course of purchases made with debit cards and credit cards during the Class Period.

93. Payment by debit or credit card increasingly is a necessity for consumers. Lack of such means of payment increasingly limits their purchase options and bargaining power.

94. Increasing reliance on electronic means of payment and other recording of personal identity and financial data has left consumers increasingly susceptible to personal data and identity theft, the adverse consequences of which also are of increasing severity.

95. Safeguarding private and confidential data of others in their possession is solely within the control of the recipients of that data, who are best able to distribute the cost of maintaining the security of that data and the consequences of the breach of such security.

96. Plaintiffs and Class members confided and entrusted their private and confidential financial and personal information to Defendant solely for the purpose of effectuating payment for purchases made from Defendant and with the expectation that Defendant would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

97. Plaintiffs and Class members did not contribute in any way to the breach

of Defendant's information technology systems or the compromise or theft of their private and confidential financial and personal data.

98. Accordingly, Defendant should be held strictly liable for the loss and damage suffered by Plaintiffs and Class members resulting from Defendant's failure to safeguard and maintain the confidentiality of their financial and personal data.

COUNT VI - NEGLIGENCE

99. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

100. Defendant owed its customers a duty of care in the handling and safeguarding of their private and confidential financial and personal information entrusted to them for the purpose of making purchases at its stores.

101. When Plaintiffs and Class members confided private and confidential financial and personal information at Defendant's request and in order to effectuate payments to Defendant, Defendant assumed a fiduciary duty and/or confidential relationship to maintain the confidentiality of such information and to safeguard and protect it from misuse by unauthorized persons.

102. Defendant breached its duties to safeguard the private and confidential financial and personal information entrusted to it by Plaintiffs and Class members. Defendant's breaches included, but are not limited to:

i. failing to monitor its IT network for the presence of foreign software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue undetected for more than three

months;

ii. failing to encrypt internal network traffic flowing between store and processor, running point-of-sales systems that were open to attack, maintaining insecure wireless connections and/or having remote access deficiencies;

iii. failing to secure its internal network credit and debit card authorization traffic from access by malware implanted on its network;

iv. failing to take appropriate steps to identify and contain the security breach when it was first discovered; and

v. failing to appropriately limit employee access to the IT network.

103. The damages described above were the direct and proximate result of Defendant's breaches of their duty to safeguard the private and confidential financial and personal information entrusted to them by Plaintiffs and Class members.

COUNT VII - UNFAIR TRADE PRACTICES

104. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 66 as if fully set forth herein.

105. Defendant represented expressly and by implication to Plaintiffs and Class members that if they used their debit cards and credit cards to effectuate purchases at Defendant's stores, their card numbers, expiration dates, PIN numbers, and other information electronically accessed by Defendant would be kept secure and would not be exposed to theft. Beginning on or about December 7, 2007, when the security of Hannaford's information technology systems was breached, these

representations were false.

106. Between being advised by Visa on February 27, 2008 that the security of Hannaford's computer systems may have been compromised, and first disclosing the security breach publicly on March 17, 2008, Defendant, by its silence, knowingly maintained and continued these false representations.

107. Since its original announcement, Defendant has provided incomplete and misleading information about the nature and extent of the data theft and has failed to notify each customer and Class member whose data was stolen of the nature and extent of the customer's data that was stolen.

108. Defendant's false representations during the Class Period that Plaintiffs' and Class members' private and confidential financial and personal information were secure and were not exposed to theft, and their failure to accurately advise Plaintiffs and Class members on a complete and timely basis of the security breach and the nature and extent of their financial and personal data that was compromised, constituted unfair or deceptive practices under the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A *et seq.*, which prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce.

109. Plaintiffs and Class members are "persons" under the Maine Unfair Trade Practices Act. Defendant's unfair and deceptive practices occurred primarily and substantially in Maine, because Hannaford is headquartered here, decisions concerning safeguarding and protection of customer information and the disclosure of the breach of security described in this Consolidated Class Action Complaint were made in Maine, and Hannaford maintained all or a substantial part of the information

technology systems that transmitted or contained such customer information for Defendant in Maine.

110. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of these unfair and deceptive practices of Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the members of the Class, respectfully request that the Court:

A. certify this action as a class action for the purposes of final injunctive relief pursuant to Fed. R. Civ. P. 23(a) and (b)(2), and for damages pursuant to Fed. R. Civ. P. 23(a) and (b)(3), and appoint Plaintiffs as Class Representatives and their counsel as Class Counsel thereof;

B. order Hannaford to notify each Class member of exactly what private and confidential financial and personal information of each Class member was exposed to theft and was, in fact, stolen;

C. order Hannaford to provide credit monitoring to all Class members;

D. enter judgment awarding damages to Plaintiffs and Class members;

E. award damages, attorneys' fees and costs to Plaintiffs and Class members (other than those who made their purchases at Defendant's stores during the Class Period in the course of trade or commerce) pursuant to 5 M.R.S.A. §205-A *et seq.*;

D. award attorneys' fees, expenses, interest and the costs of suit; and

F. award such other and further relief as it may deem just and appropriate.

JURY TRIAL DEMAND

Plaintiffs, on behalf of themselves and the Class, demand a jury trial on all issues so triable.

Dated: October 10, 2008

/s/ Peter L. Murray
Peter L. Murray (Maine Bar No. 1135)
MURRAY, PLUMB & MURRAY
75 Pearl Street
Portland, ME 04101
Phone: (207) 773-5651
Fax: (207) 773-8023
Email: pmurray@mpmlaw.com

/s/ Lewis J. Saul
Lewis J. Saul (New York Bar No. 4468740)
LEWIS SAUL & ASSOCIATES, P.C.
183 Middle Street, Suite 200
Portland, ME 04101
Phone: (207) 874-7407
Fax: (207) 874-4930
Email: lsaul@lewissaul.com

Plaintiffs' Interim Lead Counsel

Patrick E. Geraghty, Esq. (Florida Bar No. 114920)
Geraghty, Dougherty & Edwards, P.A.
2075 West First Street Suite 100
P.O. Box 1605
Fort Myers, FL 33902
Phone: (239) 334-9500
Fax : (239) 334-8930
Email : pat@7-litigators.com

Special Florida Counsel

CERTIFICATE OF SERVICE

I hereby certify that on October 10, 2008, the foregoing Consolidated Class Action Complaint was electronically filed with the United States District Court for the District of Maine using the Court's ECF/CM filing system and will be served electronically to all registered users identified on the Notice of Electronic Filing. I further certify that a paper copy of the foregoing Consolidated Class Action Complaint will be sent today via United States First Class Mail to any non-registered users identified in the Notice of Electronic Filing.

/s/ Lewis J. Saul